**STATEMENT BY**

**DANA DEASY**

**DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER**

**BEFORE THE**

**HOUSE ARMED SERVICES COMMITTEE**

**SUBCOMMITTEE ON INTELLIGENCE AND**

**EMERGING THREATS AND CAPABILITIES**

**ON**

# "DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY, CYBERSECURITY, AND INFORMATION ASSURANCE"

**FEBRUARY 26, 2019**

**NOT FOR PUBLICATION UNTIL**

**RELEASED BY THE HOUSE ARMED SERVICES COMMITTEE**

## **Introduction**

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the current efforts underway pertaining to the Department's information technology (IT) and cybersecurity. I am Dana Deasy, the Department of Defense (DoD) Chief Information Officer (CIO). I am the principal advisor to the Secretary of Defense for information management, IT, cybersecurity, communications, positioning, navigation, and timing (PNT), spectrum management, senior leadership communications, and nuclear command, control, and communications (NC3) matters. These latter responsibilities are clearly unique to the DoD, and my imperative as the CIO in managing this broad and diverse set of functions, is to ensure that the Department has the information and communications technology capabilities needed to support the broad set of Department missions. This includes supporting our deployed forces, cyber mission forces, as well as those providing mission and business support functions.

Today, I would like to highlight key areas of the Department's digital modernization and IT reform efforts now underway. First, I will provide a general overview of the Department's cloud strategy, including the Joint Enterprise Defense Infrastructure (JEDI). Then I will provide an overview of our artificial intelligence (AI) strategy, including the standup of the Joint Artificial Intelligence Center (JAIC). Regarding command, control, and communications (C3), I will briefly highlight the important work underway regarding 5G and spectrum management. I will touch upon several key elements in the area of cybersecurity, which directly impact each of the key areas of digital modernization. Finally, I will focus in on some details of our IT reform efforts.

## Cloud

Earlier this month, the Department submitted its cloud report and strategy, in accordance with Congressional requirements. As stated in that submission, DoD will remain a multi-cloud environment with both general purpose clouds and fit-for-purpose clouds as part of the long-term cloud strategy. DoD's scale and complexity of missions require multiple clouds from multiple vendors. This initiative is part of a larger effort to modernize information technology across the DoD enterprise. A modern digital infrastructure is critical to defending against cyber-attacks as well as enabling machine learning and artificial intelligence. As outlined in the cloud strategy, moving the Department to a cloud environment will enable greater computing power at greater speed and allow for the flexibility required to meet warfighter requirements at the tactical edge.

The Joint Enterprise Defense Infrastructure (JEDI) is one of the multiple cloud efforts the DoD is pursuing to enhance lethality and strategic readiness, while enabling the warfighter to respond at the speed of operations. As I have discussed with some of you previously, it is a pathfinder, general purpose, enterprise-wide cloud. JEDI will enable DoD to learn how to implement an enterprise cloud solution, take advantage of economies of scale, and enhance data-driven decision making. JEDI will be the foundational for leveraging artificial intelligence and machine learning and contribute directly to the modernization of command, control, and communication (C3) systems.

Another key component of our cloud strategy are fit-for-purpose clouds. In situations where a general purpose cloud solution is not capable of supporting mission needs, the Department may use a fit-for-purpose commercial solution. As further described in the Cloud Strategy, these situations are specific, narrowly focused cloud initiatives that address requirements that cannot be supported by a general purpose cloud. When mission needs cannot be supported by a general purpose cloud, a mission owner will be required to submit for approval an exception brief to the DoD CIO describing the capability and why the general purpose cloud service does not support their mission. Fit-for-purpose clouds, where approved and allowed, will always enhance the DoD cloud environment and not be a detriment to it.

## Artificial Intelligence (AI)

The National Defense Strategy makes clear that the character of warfare is changing. Competitors, like Russia and China, are investing heavily in modernization and artificial intelligence to redefine the future of warfare. To maintain and increase our competitive military advantage, DoD must do the same. Last June, the Department delivered its classified AI strategy to Congress. Two weeks ago, shortly after the President signed the Executive Order on AI, we released our unclassified summary of the classified DoD strategy. The DoD AI strategy contains four key points: 1) it emphasizes the need to increase the speed and agility with which we deliver and adopt AI-enabled capabilities; 2) the value of establishing a common foundation to enable decentralized development and experimentation; 3) the importance of evolving our partnerships with industry and academia; and 4) the Department's commitment to be a global leader in the safe, lawful, and ethical use of AI technologies. The Department's strategic approach emphasizes the rapid, iterative delivery of AI and importance of using lessons learned to create repeatable processes and systems that will improve effectiveness and efficiency across the enterprise. DoD will work with partners from across the Interagency, Industry, Academia, and the international community on AI missions that support DoD's ability to ensure our nation's security.

The Joint Artificial Intelligence Center (JAIC) is the focal point for carrying out the DoD AI strategy.  JAIC will accelerate DoD's delivery and adoption of AI to achieve our global mission, while attracting and cultivating a world-class AI team.  It was established last June under the office of the DoD CIO to provide a common vision, mission, and focus to drive Department-wide AI capability delivery.  JAIC is charged with the task of accelerating and scaling the use of AI across the DoD, with emphasis on near-term execution.  The ultimate goal is to use AI to solve large and complex problem sets that span across multiple services, relying on an enterprise cloud-enabled common foundation to provide shared data repositories, reusable tools, frameworks and standards, and cloud and edge services.

The AI efforts of the JAIC and the Office of the Undersecretary of Defense for Research and Engineering (OUSD(R&E)) will complement each other.  OUSD(R&E) will provide foundational AI research and technologies that JAIC can transition to the operational environment.  In turn, the JAIC will provide operational AI insights and user results to inform OUSD(R&E) focus areas.  The AI Strategy refers to National Mission Initiatives, or NMIs, and Component Mission Initiatives, or CMIs.  NMIs are broad, joint, cross-cutting AI challenges that the JAIC will orchestrate using a cross-functional team approach.  CMIs are specific to individual components, who seek AI solutions to a particular problem.  The components will run those projects, but the JAIC will support them in a number of ways, from funding, data management, common foundation, and integration into programs of record.

## **Command, Control, and Communications (C3)**

The emergence of digital technologies has introduced new challenges to the traditional C3 landscape.  In order to take advantage of new digital capabilities and to protect our warfighters from corresponding weaknesses, we must modify and modernize our C3 systems.

C3 must enable the right communications, at the right time, to protect and enable the warfighter.

All U.S. military services, in one form or another, are beginning to transition to the concept of multi-domain operations, which requires the seamless integration across land, air, sea, space and cyber. The ability of our C3 systems and forces to exchange information and communicate effectively gives our warfighters the best capabilities to deliver the fight tonight. With new approaches, and emergence of digital technologies, victory in future conflict will in part be determined by Joint and Coalition forces' ability to rapidly share information across domains and platforms.

In order to facilitate economic growth while providing national security, DoD CIO, working closely with USD(R&E), the Federal Communications Commission (FCC) and the Department of Commerce (DoC), will play a key role in the Department’s efforts in the implementation of 5G telecommunications. As the primary federal user of spectrum, we must help guide effective implementation of the “Presidential Memorandum for Developing a Sustainable Spectrum Strategy for America’s Future.” DoD must become a key innovator in spectrum sharing technology and policy, while leveraging mutually dependent C3, cloud, cyber and AI technologies, to gain and maintain an advantage over our competitors. DoD CIO has been working closely with Federal partners and Industry through the Wireless Innovation Forum to share spectrum, and accommodate both broadband and naval radar operations in the 3550-3650 MHz band. The Department has been a key participant in shaping this innovative spectrum sharing framework.

## **Cybersecurity**

DoD released the 2018 Cyber Strategy this past September. As aligned with the National Cyber Strategy, the Department of Defense Cyber Strategy articulates how DoD implements the National Defense Strategy in cyberspace, describes how the Department aims to compete, deter, and win alongside allies and partners in cyberspace, and directs DoD to defend forward, shape the day-to-day competition, and prepare for war.

As I testified before the Senate Armed Services Committee, Subcommittee on Cybersecurity last month, the DoD CIO, working closely with the Defense Information Systems Agency (DISA) and the Principal Cyber Advisor (PCA), implements the DoD Cyber Strategy in close coordination with the Military Departments and other DoD Component CIOs. DoD CIO and PCA co-lead bi-weekly meetings focused on cyber issues with the Deputy Secretary of Defense and all of the Military Departments and Office of the Secretary of Defense (OSD) Principals present. These meetings ensure that the Deputy Secretary of Defense is kept abreast of progress on cyber initiatives and that all Department leaders are present to receive direction and share challenges. Additionally, DoD CIO also works closely with the Protecting Critical Technology Task Force to identify technical solutions to enhance protections of the Defense Industrial Base (DIB).

The Department has created the "Cyber Top Ten", which helps us to prioritize where and how we apply resources and innovation to execute our Cyber Strategy. The "Cyber Top Ten" focuses on remediation strategies for a complex cyber landscape, whose components range from information and networks, to our cyber workforce and supply chain risk management, and beyond.

For the first time, DoD CIO is reviewing, commenting on, and certifying all of the IT budgets, which include cyber, across the Department. DoD CIO's Congressionally mandated responsibility to certify the Military Departments' cybersecurity investments and efforts enables me to ensure the Department is pursuing enterprise cybersecurity solutions that are lethal, flexible, and resilient.  DoD CIO now has the authority to set and enforce IT standards across the Department.  Standards are not limited to the technical standards developed by the commercial sector and organizations like the International Standards Organization.  Standards include setting the bar for cybersecurity requirements, such as endpoint security standards and standards for architecture, and DoDIN standards.

The Department’s cyber workforce is critical to our mission success.  The authorities provided by Congress have allowed the Department to adjust existing personnel policies and to implement new policies that account for this dynamic need in an increasingly important mission area.  One key authority being the establishment of the Cyber Excepted Service (CES).  By fostering a culture based upon mission requirements and employee capabilities, CES will enhance the effectiveness of the Department’s cyber defensive and offensive mission.  This will provide DoD with the needed agility and flexibility for the recruitment, retention and development of high quality cyber professionals.

## Information Technology (IT) Reform

DoD CIO is working closely with the Chief Management Officer (CMO) to achieve a modernized and effective force through DoD-wide IT reform activities.  These activities are being established to implement, consolidate, and streamline capability delivery to support an evolving mission environment.

Establishing a consolidated and converged IT infrastructure drives efficiencies across the Department, and provides opportunities for reductions in acquisition overhead, an increase in combined purchasing power, and the utilization of shared expertise across the DoD environment. Refocusing IT manpower initiatives towards an increase in experience and skillsets, coupled with automation improvements, provides a reduction in labor resources that can be aligned to support emerging mission areas. Standardizing and modernizing the IT environment eliminates unnecessary systems, and allows the DoD to focus finite cyber resources across fewer areas, ultimately shrinking the Department's cyber threat attack surface.

Several key reform efforts are underway. First, Network and Service Optimization Reform will converge DoD networks, service desks and network/service operation centers into a consolidated, secure, and effective environment capable of addressing current and future mission objectives. Second, Cloud & Data Center Optimization Reform transitions the DoD to a cloud-enabled future. Enterprise Collaboration/IT Tools Reform converges and transitions the DoD collaboration capabilities into a unified commercial cloud-enabled enterprise service. Finally, License Consolidation Reform negotiates improved terms and conditions with commercial vendors, prioritizes IT spend across the department, and standardizes purchasing processes.

## **Conclusion**

I want to emphasize the importance of our partnerships with Congress in all areas, but with a particular focus on digital modernization and IT reform. The increased authorities that have been granted to the DoD CIO with each National Defense Authorization Act are one key example of this partnership. Continued support for a flexible approach to cloud, AI, C3, and cyber resourcing, budgeting, acquisition, and personnel will help enable success against an everchanging dynamic threat environment.  I look forward to continuing to work with Congress in these critical areas.  Thank you for the opportunity to testify this afternoon, and I look forward to your questions.